Claims:

1. A method of authenticating an end-user client in a computer-based communication system comprising the steps of:

   a) sending, by the end-user client, an authenticating domain identifier to an authentication server;

   b) creating, by the authentication server and depending on the authentication domain identifier, an authentication stack comprising one or more stack entries;

   c) rendering, for each stack entry and depending thereon, an authentication service to produce an authentication result for that entry; and

   d) consolidating authentication results to obtain an authentication status for the end-user client.

2. The method as defined in claim 1 wherein the authentication identifies an application ID.

3. The method as defined in claim 2 wherein the authentication server, dependent on the application ID, retrieves a configuration specifying authentication application, which configuration is used for creating the authentication stack.

4. The method as defined in claim 1 wherein the authentication service includes local and remote services.

5. The method as defined in claim 4 wherein the local and remote services include but are not limited to biometric schemes, cryptographic hardware services, smart cards and USB tokens.

6. The method as defined in claim 1 wherein responsive to an authentication status corresponding to a successful authentication, a unique session ID is sent to the end-user client.

7. A system for authenticating an end-user client in a computer-based communication system comprising:

means, at the end-user client, for sending an authenticating domain identifier to an authentication server;

means, at the authentication server and depending on the authentication domain identifier, for creating an authentication stack comprising one or more stack entries;

means for rendering, for each stack entry and depending thereon, an authentication service to produce an authentication result for that entry; and

means for consolidating authentication results to obtain an authentication status for the end-user client.

8. The system as defined in claim 7 wherein the authentication identifies an application ID

9. The system as defined in claim 8 wherein the authentication server, dependent on the application ID, retrieves a configuration specifying how to create the authentication stack.

10. The system as defined in claim 7 wherein the authentication service includes local and remote services.

11. The system as defined in claim 7 wherein the local and remote services include biometric schemes, cryptographic hardware services, smart cards and USB tokens.

12. The system as defined in claim 7 wherein responsive to an authentication status corresponding to a successful authentication, a unique session ID is sent to the end-user client.